Product:	PowerShare™ Network	**Doc. Num:**	PSNA012c
Version:	All versions	**Date:**	22 March 2018
Subject:	SSO Technical Specifications		

Overview

The Nuance *PowerShare Network* solution enables single sign-on (SSO) for its Facility users who have access to the application from their existing SAML2 Identity provider or Active Directory system. The solution supports the SAML 2.0 authentication scheme for both its web-based and mobile applications.

The API and web widgets are not impacted by this new authentication/authorization scheme.

Definitions

Security Assertion Markup Language (SAML): An XML based, open standards data format for exchanging authentication and authorization data between two systems: the Identity Provider (IdP) and the Service Provider (SP). The protocol uses security tokens containing assertions to pass information about a user between a SAML authority (an Identity Provider) and a SAML consumer (a Service Provider, such as the Nuance *PowerShare Network*).

Identity Provider (IdP): A SAML authority responsible for providing identifiers to users who want to interact with a system, and notifying the system that the identifier presented by a user is known to the provider. It also provides other user information about the user that is known to the provider.

Service Provider (SP): An application to which a user requests access. For our purposes here, the Nuance *PowerShare Network* solution is a Service Provider (SP).

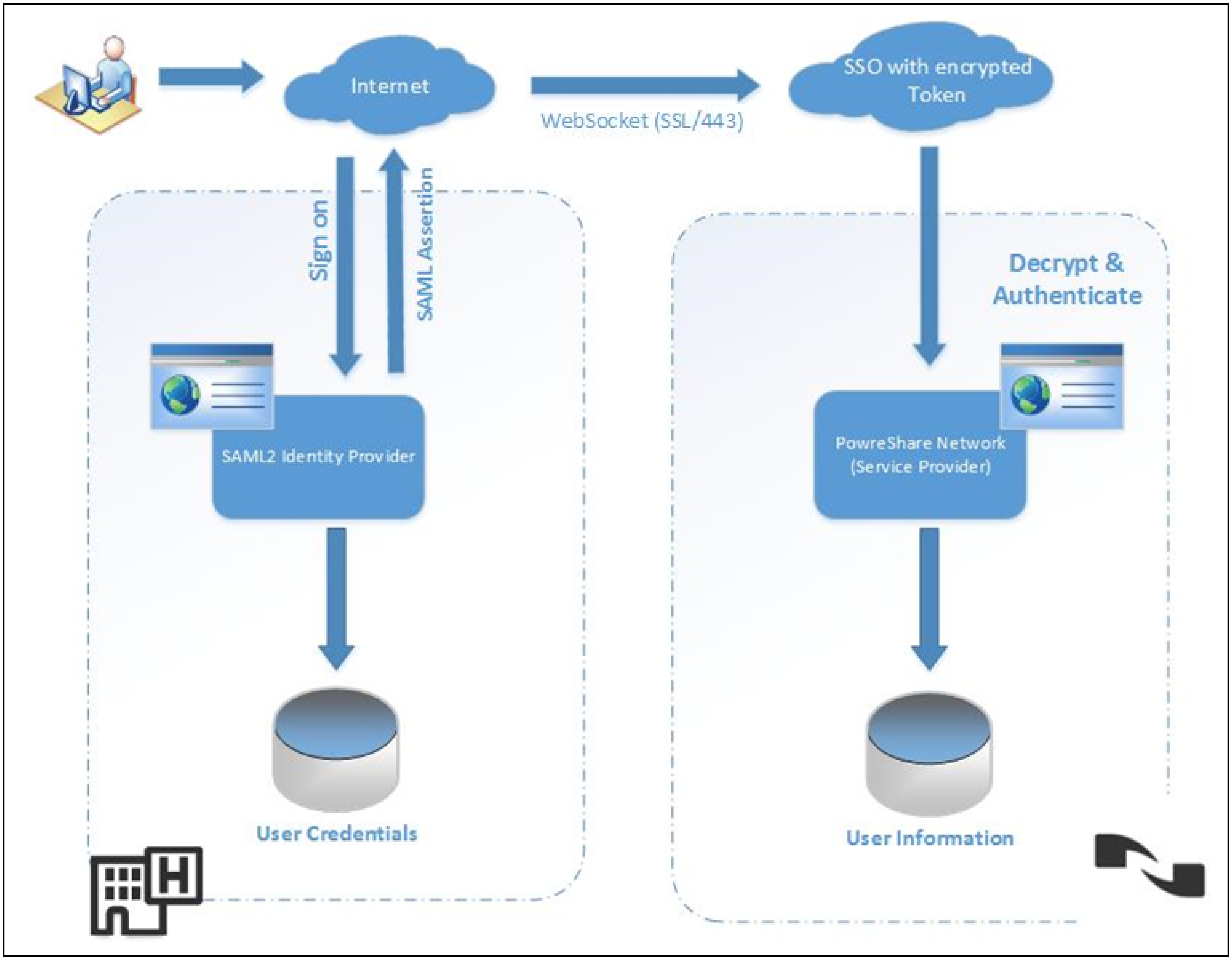
Responsibilities: Facility and Nuance

1. **Nuance and the facility** agree upon the configuration parameters.
2. **Nuance Support** provides the SAML meta data to the facility IT team.
3. **The facility** adds the *PowerShare Network* application to the SAML IdP system.
4. **The facility** provides a Signing and Encryption certificate (if required) to Nuance.
5. **Nuance and the facility** configure the facility's IdP system and SP with the required attributes.
6. **Nuance IT Operations** adds the facility account into its SSO solution.

Architecture

Option #1: Facility with a SAML2-Compliant Identity Provider

The illustration below depicts SSO communication between *PowerShare Network* and a hospital network. The Identity Provider is a SAML2-compliant system.



Process

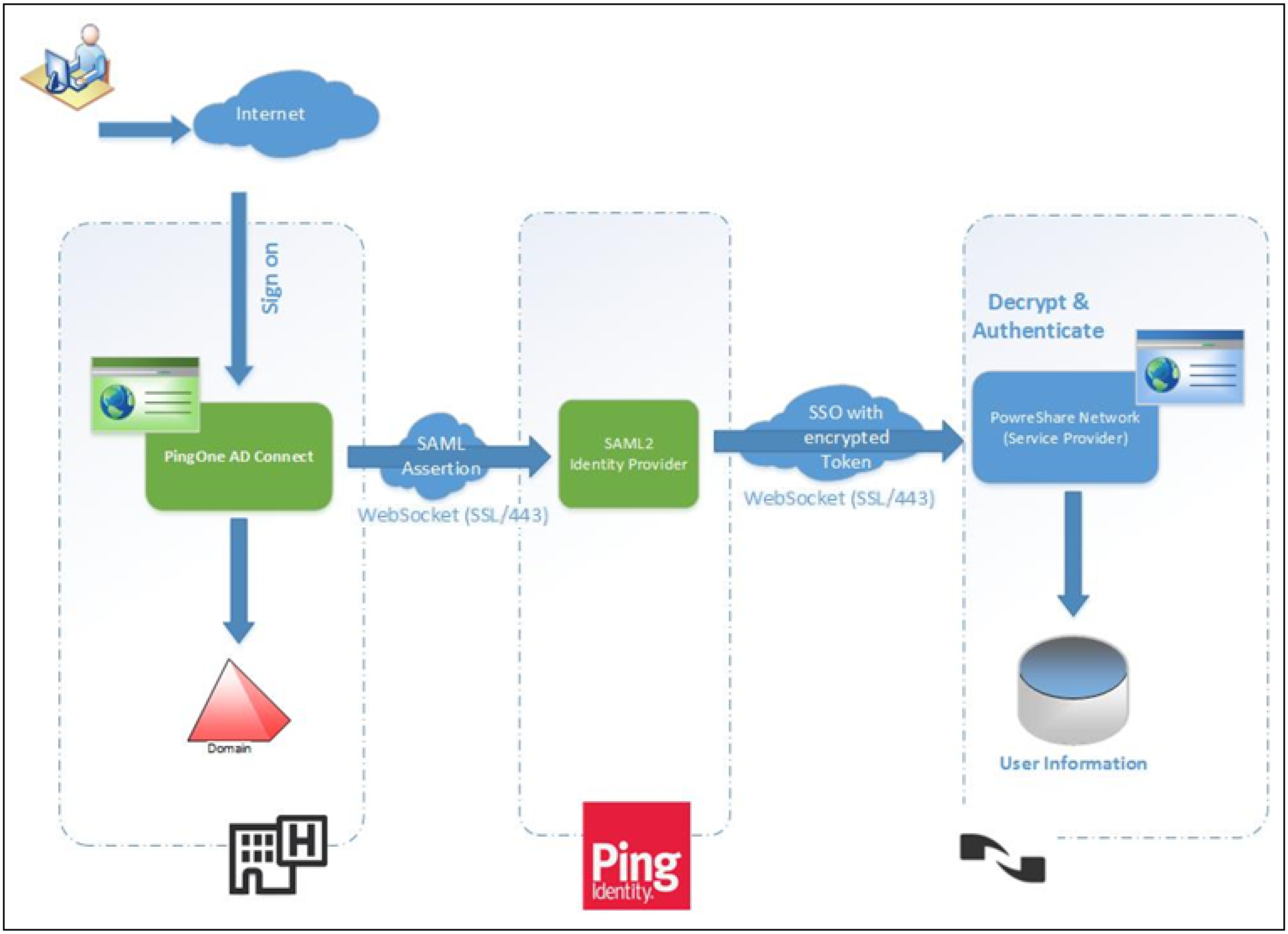
1. The user navigates to a private-labeled *PowerShare Network* URL and is seamlessly redirected to the Institution Identity Provider login page.
2. The user logs in with their Facility-based user name and password.
3. The SAML2 Identity Provider generates a SAML2 assertion with the required data attributes of the user and sends this to the *PowerShare Network* Service Provider.
4. The *PowerShare Network* Service Provider decrypts and authenticates the SAML assertion and redirects the user to the *PowerShare Network* application.

Option #2: Facility Has Active Directory (No SAML2-Compliant Identity Provider System)

Nuance suggests the third-party SAML solution from PingOne (https://www.pingidentity.com/en/products/pingone.html) to enable SSO for a facility with a non-SAML compliant system that uses Active Directory. PingOne is a cloud based SSO solution that allows users to sign on to all of their applications with a single user name and password.

For Active Directory, you can use the PingOne AD Connect Utility to establish SSO between the Nuance *PowerShare Network* and your Active Directory. This allows your facility administrators to manage their users and have them sign into *PowerShare Network* with the same user name and password they use everywhere else within your institution.

The illustration below shows an example of the AD/no SAML2-compliant type of setup.



PingOne AD Connect with IIS uses the SAML 2.0 protocol to communicate with PingOne. It uses a secure back channel protocol to communicate with PingOne. This is an inbound/outbound connection on port 443. No other external access to the AD Connect host is necessary. With AD Connect you do not need to open ports in a firewall, install IIS, or employ signing certificates. You can optionally use Integrated Windows Authentication (IWA) as the authentication protocol on your network. High availability (automatic failover and load balancing) is handled by the PingOne data centers, and requires no configuration or management on your part.

AD Connect connects to PingOne using a WebSocket secure connection on port 443, and authenticates PingOne using SSL. PingOne authenticates the requesting AD Connect instance using the digital signature. No SSL certificate is needed on the AD Connect side. This connection is used for full-duplex communications between PingOne and AD Connect services.

The PingOne authentication request sent to AD Connect is a token that contains the username and password encrypted with the public key of the selected AD Connect instance. PingOne sends the request to AD Connect using a WebSocket back channel. Only the intended AD Connect instance can decrypt the request token. AD Connect then validates the username and password with Active Directory and sends a response token back to PingOne. The response tokens are valid for a single use only.

The server hosting the AD Connect software has to be configured in the same Active Directory domain controller environment.

Process

1. The user navigates to a private-labeled *PowerShare Network* URL and is seamlessly redirected to the PingOne AD Connect web login page.
2. The user logs in with their facility-based user name and password.
3. The user is then redirected by the PingOne SAML2 Identity Provider, which generates a SAML2 assertion containing the user's required data attributes, and sends the information to the *PowerShare Network* Service Provider.
4. PowerShare Network Service Provider decrypts and authenticates the SAML assertion and redirects the user to the *PowerShare Network* application.

Click the links below for more information on PingOne AD Connect Software.

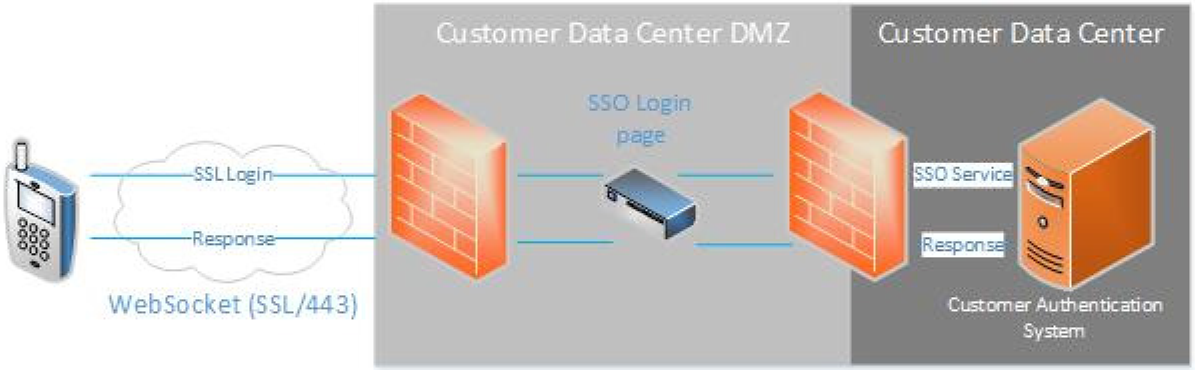
How AD Connect Works

Secure Your AD Connect with IIS Deployment

Mobile Architecture

For customers whose SSO login page is hosted within its network firewall, the Mobile application cannot be accessed outside the network. In order to access the mobile application from outside the network, the SSO login page must be hosted in the Customer's Data Center DMZ environment.

The illustration below depicts the communication flow from the Mobile device and Customer's SSO login page.



Data Attributes

The following data attributes are included in the SAML assertion and used to identify the user in the *PowerShare Network* solution.

Name	Data Type (number of characters)	Required (R) or Optional (O)	Description
Email Address	Text (101)	R	Facility user Email address. The email ID is used as a unique primary ID to linked to PowerShare Network account
First Name	Text (101)	R	First name of the user
Last Name	Text (101)	R	Last name of the user
Role	Text (10)	O	Identifies the role of the user in the *PowerShare Network* solution. **ADMIN**, **CLERK**, and **PHYSICIAN** are the only possible values
National Provider Identifier (NPI)	Number (10)	R/O (see Description)	A unique National Provider Identifier (Required if the user's role is **PHYSICIAN**)

Workflows

When a Facility account is enabled for SSO, the facility can no longer add or update its users using the *PowerShare Network* application. All of the facility's users (except for **Stat/Temp** users) will be provisioned using their SSO logins. You are allowed to change the user role for the facility's Owner Admin account. You can still add **Stat/Temp** users in the *PowerShare* web application.

The following SSO workflows are supported by the *PowerShare Network* solution.

Login

The user accesses their facility login web page to sign into the *PowerShare Network* solution. After a successful login the user is redirected to the *PowerShare* application. The solution supports only a Service Provider (SP)-initiated login.

In the *PowerShare* Mobile application, the user is redirected to their facility's login page (based on their email address).

Account Provisioning

After a successful login for a user who does not exist in the *PowerShare Network* solution, the service adds the user based on the **Role** specified in the data attributes of the SAML assertion.

If the **Role** and **NPI** values are not present in the IdP system, the *PowerShare* application will inquire if the logged in user is a Physician.

- If the user **is not** a Physician, they will be provisioned as a **Clerk**. Facility primary administrators can modify the user role to **Admin** if required.
- If the logged in user **is** a Physician, they will **not** be provisioned. A facility administrator must add the physician using a comma separated value (csv) file containing the Physician data.

This workflow is **not** supported from the *PowerShare* Mobile Application. The user's email address identifies the user as an SSO user and redirects the user to a login web page for its login credentials. The user is then redirected back to the mobile application.

Update

When a user whose role or name has been changed successfully, the *PowerShare Network* system updates the user's profile with the appropriate new values and logs the user in. If the user's role has changed, the system will change the user's role in the *PowerShare* application.

If no **Role** information is available, the user's role in the *PowerShare* application will ***not*** be impacted.

Logout

When the user logs out of the *PowerShare Network* solution, it only triggers a successful logout from the *PowerShare* application and does ***not*** log out the user from the facility IdP-initiated logout. In addition, the solution does ***not*** support a single logout (SLO) profile, which enables a user to log out of all the participating applications in a federated session nearly simultaneously.

Access Management

Because of the account auto-provisioning workflow describe above, by default, **all** user logins will have access to the *PowerShare* application. In order for customers to allow only specific users to access the application, customers will have to implement the access restriction policy in their SAML system.

PowerShare does not know which users to provision. The SAML system allows you to restrict access to a specific group of users by applying its group level or individual user restrictions to the *PowerShare* application's URL.

Specifications

Item	Description
Protocol Version	SAML version 2.0
Target URL	https://www1.nuancepowershare.com/smr/sso?partner=**<Nuance-provided unique label>**
Service Provider SAML 2.0 Entity ID	https://sso.nuancepowershare.com
Assertion Consumer Service (ACS)	https://sso.nuancepowershare.com/sp/ACS.saml2
Meta Data	<Provided by customer> URL or file
SAML Binding	Post and/or Redirect (*NOTE: Artifact and SOAP are not supported at this time.*)
IdP Entity ID	<Provided by customer>
IdP SSO Service URL (POST / REDIRECT)	<Provided by customer>
Attribute Contract (Names)	<Provided by customer>
Single Logout Endpoint	<Provided by customer>
Signature Policy	
Sign AuthnRequest over Post and Redirect Binding?	Yes or No
Require Signed SAML Assertions?	Yes or No
Encrypt Assertion?	Yes or No
Encrypt the SAML subject in SLO messages to the IdP?	Yes or No
Encrypt Name Identifiers?	Yes or No
Signing certificate	<Provided by customer>
Encryption Certificate	<Provided by customer or by PowerShare Network support>
Signing Algorithm	Choices are: RSA SHA256 RSA SHA1 RSA SHA384 RSA SHA512